Admin's Guide

Nokia Mobile VPN Client

for Symbian devices

October 2010

NOKIA

Nokia for Business

Table of Contents

1 About This Document ... 3
1.1 Scope ... 3
1.2 References ... 3
2 Compatible devices and gateways ... 3
2.1 Compatible Nokia devices ... 3
2.2 Compatible VPN gateways ... 3
3 Introduction ... 4
3.1 What is a VPN ... 4
3.2 How does a VPN work ... 4
3.3 What is Nokia Mobile VPN Client ... 5
3.4 Key Features ... 5
3.5 Supported Standards ... 6
3.6 Key Concepts ... 6
4 Deployment of Nokia Mobile VPN ... 7
4.1 Important Safety Notes ... 7
4.2 System Requirements ... 7
4.3 Deployment steps ... 7
5 Installation of Nokia Mobile VPN Client ... 7
6 Configuring Nokia Mobile VPN Client ... 9
6.1 Creating VPN configuration file ... 9
6.2 Configuring Nokia Mobile VPN Client Via the Device User Interface ... 9
6.3 Configuring Nokia Mobile VPN Client with OMA Device Management ... 15
6.4 Configuring with Nokia Security Service Manager ... 17
7 Using Nokia Mobile VPN Client ... 19
8 Frequently Asked Questions ... 20
9 Troubleshooting ... 20
9.1 How to Get Support ... 20
9.2 VPN Log ... 20
9.3 Error codes ... 20
10 Glossary ... 22

1 About This Document

This document is an administrator's guide for Nokia Mobile VPN Client.

There are different Mobile VPN Client versions available:

- Version 3.1 is compatible with Nokia Symbian S60 3rd Edition, Feature Pack 1 devices
- Version 4.0 is compatible with Nokia Symbian S60 3rd Edition, Feature Pack 2 and S60 5th Edition
- Version 4.2 is compatible with Nokia Symbian¨3 devices

See [9] for list for devices of each Symbian OS edition.

This guide introduces the main features, and discusses the deployment and configuration of Nokia Mobile VPN client.

1.1 Scope

The document is structured as follows:

- Chapter 1, About This Document
- Chapter 2, Compatible devices and gateways
- Chapter 3, Introduction to VPN and Nokia Mobile VPN Client
- Chapter 4, Deployment
- Chapter 5, Installation
- Chapter 6, Configuration
- Chapter 7, Using Nokia Mobile VPN Client
- Chapter 8, Frequently Asked Questions
- Chapter 9, Troubleshooting
- Chapter 10, Glossary

1.2 References

Reference	Description
[1]	Nokia for Business, http://www.nokia.com/mobilevpn
[2]	Nokia Support / Download Software, Nokia Mobile VPN, http://europe.nokia.com/support/download-software/nokia-mobile-vpn
[3]	Nokia Mobile VPN Client Policy Specification, downloadable in [2]
[4]	Nokia Mobile VPN Client OMA DM Specification, published by Forum Nokia http://www.forum.nokia.com/Tools_Docs_and_Code/Documentation/Device_Management/OMA_DM_Management_Objects.xhtml
[5]	PKI Management OMA DM specification, published by Forum Nokia http://www.forum.nokia.com/Tools_Docs_and_Code/Documentation/Device_Management/OMA_DM_Management_Objects.xhtml
[6]	Nokia Security Services Manager Administration Guide, v3.0.1, Part No. N450778006 Rev A, Nokia 2005 https://support.nokia.com
[7]	Nokia Security Service Manager Installation Guide, v3.0.1, Part No. N450783006 Rev A, Nokia 2005 http://support.nokia.com
[8]	Nokia Mobile VPN Client Policy Tool, http://europe.nokia.com/support/download-software/nokia-mobile-vpn/compatibility-and-download
[9]	Device Specifications, Forum Nokia http://www.forum.nokia.com/devices/matrix_s60_1.html

You might also need to refer to

- Your Nokia device's user guide
- Documentation of your corporate compatible device management solution

2 Compatible devices and gateways

2.1 Compatible Nokia devices

Nokia Mobile VPN is pre-installed in Nokia Eseries devices, e.g. Nokia E51, E52, E55, E63, E66, E71, E72, E75 and E7.

To other Nokia devices based on Symbian OS, Nokia Mobile Client can be downloaded in [2].

Note: The screen layouts of different devices might differ from those presented in this document.

2.2 Compatible VPN gateways

The following VPN gateways have been used as the main gateways in the interoperability testing of Nokia Mobile VPN Client:

- Check Point NGX R65
- Nokia IP VPN v6.3

- Cisco VPN 3000 Concentrator series v4.7.2
- Cisco ISR
- Cisco ASA
- Alcatel-Lucent Brick

Documents describing how to configure the gateways to ensure compatibility with Nokia Mobile VPN Client are available at [2].

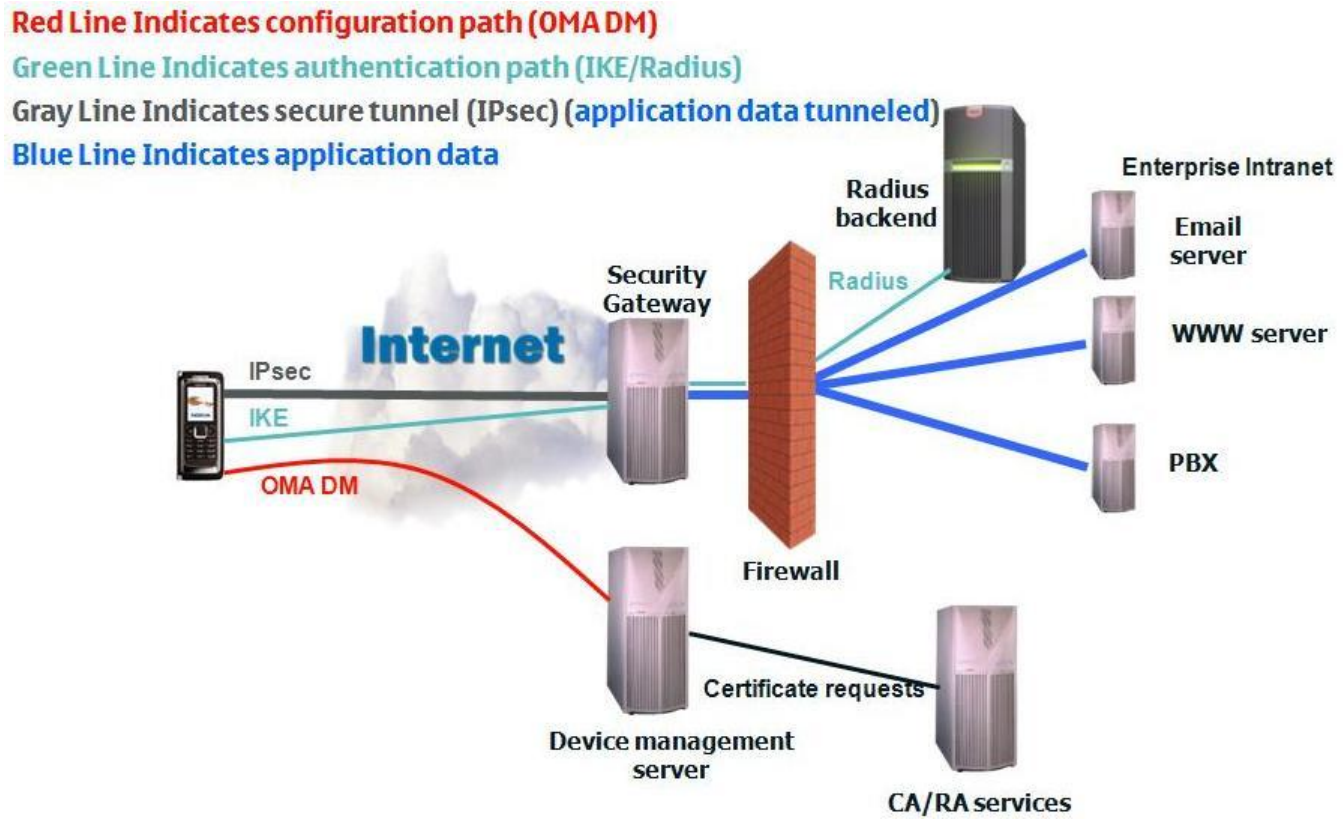
In addition, some tests have been run with the following VPN gateways:

- Nokia Siemens Networks I-WLAN Solution
- strongSwan (http://www.strongswan.org)

3 Introduction

3.1 What is a VPN

A Virtual Private Network (VPN) is a security-protected data tunnel that runs on an existing unsecured network—like the public Internet or wireless networks. VPNs may be used to cost-effectively and securely communicate between corporate sites or between remote users and a corporate network.



3.2 How does a VPN work

Virtual Private Network (VPN) enables remote devices to have encrypted and authenticated communications with enterprise networks through the mobile network and Internet.

VPN gateways are used to encrypt data entering the VPN tunnel, and decrypt data leaving the VPN. Since the VPN maximizes confidentiality, integrity, and authenticity, sensitive corporate data can travel more securely over a public network like the Internet.

VPN provides:

- Authentication - ensures the identity of all communicating parties
- Authorization and access control
- Confidentiality - encryption of data delivered via VPN connection
- Integrity - ensures that data is not altered in any way during transit

A common use of a VPN is to allow remote users access to corporate network resources. User can for example

- Use browser to access company's Intranet web pages
- Access corporate emails
- Have encrypted VoIP voice calls to other corporate users

A remote user first establishes a VPN connection between the device and the VPN gateway. Once the VPN connection is established, the remote user can securely access private network resources on their corporate network.

3.3 What is Nokia Mobile VPN Client

Nokia Mobile VPN Client is an interoperable and manageable IPsec VPN client that extends corporate networks to mobile devices that are optimized for business use and offers secure access to business applications.

Applications see VPN client as normal Symbian OS Access Point and there is no need to implement any special support to application to make it be able to benefit VPN functionality.

Applications running in a Symbian device use VPN services through VPN access points. Associating an ordinary Internet Access Point (IAP) or a Network destination with a security policy creates a VPN access point. As far as applications are concerned, VPN access points behave similarly to ordinary Internet Access Points. For instance, the user selects the VPN access point used by an application with the same user interface that is used to select ordinary Internet Access Point. If an application is configured to use a VPN access point, the VPN Client Application will start up automatically when the application starts using the network services through the access point. VPN Client application will, at that point, handle the user authentication and set up the connection through the VPN gateway according to the security policy of the VPN access point. Once the authentication and connection setup has been completed successfully, all IP traffic through the VPN access point will be encrypted. The VPN access points make use of the VPN transparent to applications. Applications that do not need VPN access can be used at the same time simply by configuring them to use ordinary Internet Access Points. This means that, for example, browsing and accessing email can be done through the enterprise network using VPN services at the same time as Multimedia Messaging and IM Chat communicate directly over GPRS with the servers of the network operator. Note: This behavior is limited by the number of simultaneous PDP contexts that the network of the device supports, and also depends on the VPN policy configuration.

Nokia Mobile VPN client works transparently on the IP layer, which allows seamless use of mobile applications. It supports many authentication methods, for example shared secret, one time password and PKI-based authentications, and SIM/USIM-based authentication for mobile operator environments.

Central management of security policies and updates over the air provide an uninterrupted service to mobile workers. VPN Client can be configured via the Open Mobile Alliance Device Management (OMA DM), see [4] and [5], or Windows PC using Nokia Mobile VPN Policy tool.

VPN Client can also be installed via OMA DM.

3.4 Key Features

The key features include the following:

Feature:

- Integration to Internet access point selection using VPN access points
- Integration to Network destination selection
- Support for IPsec over Network Address Translation (NAT)
- Split-tunneling
- Internal addressing and DNS
- Automatic policy loading and certificate enrollment via Nokia Security Services Manager (Not supported version 4.2 onward)
- Automatic policy loading and certificate enrollment via OMA DM
- Intranet network destination (version 4.0 onward)
- When installing VPN policy from a file through the device's user interface, VPN access point is automatically created under Intranet network destination (version 4.0 onward).
- Provisioning of VPN policy from Microsoft Windows 2008 R2 server, which includes a built-in security gateway called Agile VPN (supported version 4.2 onward)

Encryption algorithms:

- DES (56 bit), 3DES (168 bit), AES (128, 192, 256 bit) encryption
- SHA1, MD5 hash algorithms for encryption

User authentication:

- X.509v3 digital certificates for authentication and certificate chains
- CRACK (Challenge/Response Authentication for Cryptographic Keys) for legacy authentication
- Username/Password
- Token cards
- IKE pre-shared secret
- xAuth – Extended authentication. Version 4.2 onward silent xAuth supported (Username and password queried only once)
- DSA certificates
- RSA Public Key Encryption, RSA Revised Encryption
- GSM Subscriber Identity Modules (SIMs) via EAP-SIM
- Third Generation authentication and key agreement via EAP-AKA (requires USIM application on the smart card)
- Silent authentication with username and password, IKE pre-shared keys
- Silent authentication with client certificates

Key exchange algorithms:

- Diffie-Hellman 768-1536 bit (Groups 1, 2, 5 and 14).

Key management:

- IKE (ISAKMP/Oakley) (main, aggressive)
- PKCS#8 for Private Key Format
- PKCS#5 v2 for Private Key Encryption
- PKCS#12 for importing Private Key and Certificate
- Perfect Forward Secrecy (PFS) for IPsec associations
- IKEv2

3.5 Supported Standards

Nokia Mobile VPN client supports the following IETF specifications from applicable parts. The list of the specifications below is non-exhaustive:

- RFC2401 Security Architecture for the Internet Protocol
- RFC2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC2405 The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC2406 IP Encapsulating Security Payload (ESP)
- RFC2407 The Internet IP Security Domain of Interpretation for ISAKMP
- RFC2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC2409 The Internet Key Exchange (IKE)
- RFC2410 The NULL Encryption Algorithm and Its Use With IPsec
- RFC2451 The ESP CBC-Mode Cipher Algorithms
- RFC3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange
- RFC3947 Negotiation of NAT-Traversal in the IKE
- RFC3948 UDP Encapsulation of IPsec ESP Packets
- RFC4186 Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)
- RFC4187 Extensible Authentication Protocol Method for Third Generation Authentication and Key Agreement (EAP-AKA)
- RFC4301 Security Architecture for the Internet Protocol
- RFC4306 Internet Key Exchange (IKEv2) Protocol

3.6 Key Concepts

The following table describes the most important terms and concepts used in this document.

Concept	Description
VPN Policy	A VPN policy is a pair of text files (.pin and .pol) that describe the organization's policy (security parameters) for remote access VPN. The format of the policy file is specified in [3]. You can create VPN policy files with Nokia Mobile VPN Policy Tool. The policy files define, for example, the IP address or Fully Qualified Domain Name (FQDN) of the VPN gateway, Internet Key Exchange parameters and algorithtms, and IPsec parameters and algorithms.
VPN access point	In Symbian devices, connection settings are represented as Internet access points. There are internet access points e.g. for packet data connections and WLAN connections. Similarly, Nokia Mobile VPN connections are shown as VPN access points. A VPN access point is associated with a VPN policy and an underlying bearer Internet access point, which will be used for the VPN connection. To use a VPN connection in an application, a VPN access point will suffice instead of, for example, a packet-data access point.
CA certificate	In most cases, Nokia Mobile VPN client authenticates the VPN gateway based on a Certificate Authority (CA) certificate, which needs to be installed in the device. The VPN policy refers to the CA-certificate that is used by the oganization's VPN gateways. A CA certificate can be brought to the device from a file via the device user interface, or with a device management solution. Certificates must be in the DER-encoded X509.3 ASN.1 format. A VPN CA certificate is not required if IKE pre-shared key authentication is used.
Client certificate	Client certificates are one of the supported client authentication methods of Nokia Mobile VPN client. A client certificate is associated with a key pair that consists of a public key and a private

	key. To use certificate based authentication, the device needs to have a key pair and a corresponding client certificate that is signed by a Certificate Authority that the VPN gateway trusts. A client certificate can be brought to the device through the device user interface, together with the associated key pair, in a PKCS#12 file. Client certificates and key pairs can also be managed with OMA DM. In addition to PKCS#12, the OMA DM supports a procedure where the device generates a key pair and requests a client certificate for the public key using a PKCS#10 format.
User key store Device key store	Private keys are stored either in a user key store or a device key store. When a private key that is stored in the user key store is used, the device authorizes the use of the key from the user by prompting for the user key store password. The minimum length for the password is 6 characters. The device can use the keys stored in the device key store automatically, without prompting any passwords from the user.
User key store password	The user key store password protects the user key store. When a key stored in the user key store is used, the device prompts the user to enter the key store password. The user can set the password locally through the user interface on the device.
VPN configuration file	VPN configuration file is a zip file with extension .vpn. A VPN policy, command file for setting device lock, certificates, and private keys can be bundled into a single file, which can be imported through the device's user interface. This reduces several manual steps when setting up the VPN client via the device user interface, since the user does not need to import a CA certificate, private keys, and a VPN policy file separately. The private key will be automatically placed either in the device key store or in the user key store, as required in the VPN policy. VPN configuration file can be created with Nokia Mobile VPN Policy Tool. The policy file and command file formats are specified in [3].

4 Deployment of Nokia Mobile VPN

This chapter describes the system requirements and the deployment process.

4.1 Important Safety Notes

The safety instructions in the user guides that accompany your device apply when using Nokia Mobile VPN client.

4.2 System Requirements

To install and use Nokia Mobile VPN client, you need the following:

- A compatible Nokia device, see chapter 2 for details.
- A VPN gateway compatible with Nokia Mobile VPN client, see chapter 2 for details.
- A VPN configuration file, see Chapter 6 for more information.
- (Optional) Certificate, which are required for other authentication methods besides IKE pre-shared keys
- (Optional) A device management solution for configuring Nokia Mobile VPN client

4.3 Deployment steps

As Nokia Mobile VPN client connects to your organization's intranet, you need to have the correct settings for your organization's environment.

For taking Nokia Mobile VPN Client into use you have to go through the following steps:

- Configure the VPN gateway if necessary. Simplified configuration instructions for some security gateways can be found in http://europe.nokia.com/support/download-software/nokia-mobile-vpn. We recommend though to use the configuration guides provided by the gateway vendor.
- Install Nokia Mobile VPN client on your compatible Nokia device if it is not pre-installed already.
- Create VPN configuration file. This step can be skipped if your company has Nokia Security Services Manager used for device management.
- Install the configuration file to the Nokia device.

5 Installation of Nokia Mobile VPN Client

VPN client is pre-installed in Nokia E-series devices and for them this step is not needed.
If you have some other compatible Nokia device (see chapter 2.1) you have to install the VPN Client to your device. If VPN is already installed in your device, you can upgrade to a newer version if desired.

If there is no VPN installed in your device, you can download it in Support / Download software web page [2].
The VPN client can be installed as any Symbian S60 application. There are several ways to do it. The easiest way is to go to the web site mentioned above, select your device and click the file link and the installation starts.

You can also download the installation file first to your PC and then move it to the device by using Bluetooth or USB, or you can use Nokia PC Suite to install the application.

An example of how to install Nokia Mobile VPN client application (SISX file) is illustrated in the following steps:

1. Transfer the SISX file to the device via Bluetooth, USB, or Infrared, or use a memory card.

2. Install Mobile VPN client to device memory or a memory card by opening the file from the file manager or messages.

3. In the confirmation query shown in Figure 1, press "Yes." Then, a progress note is displayed during the installation. Follow the instructions on screen.

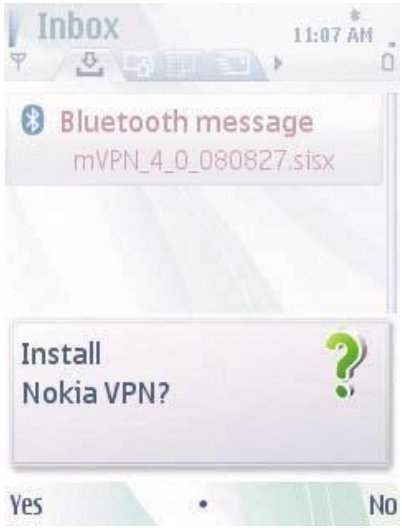


Figure 1 Installing Nokia Mobile VPN from messaging

4. For all three installation detail dialogs shown in Figure 2, press Continue.

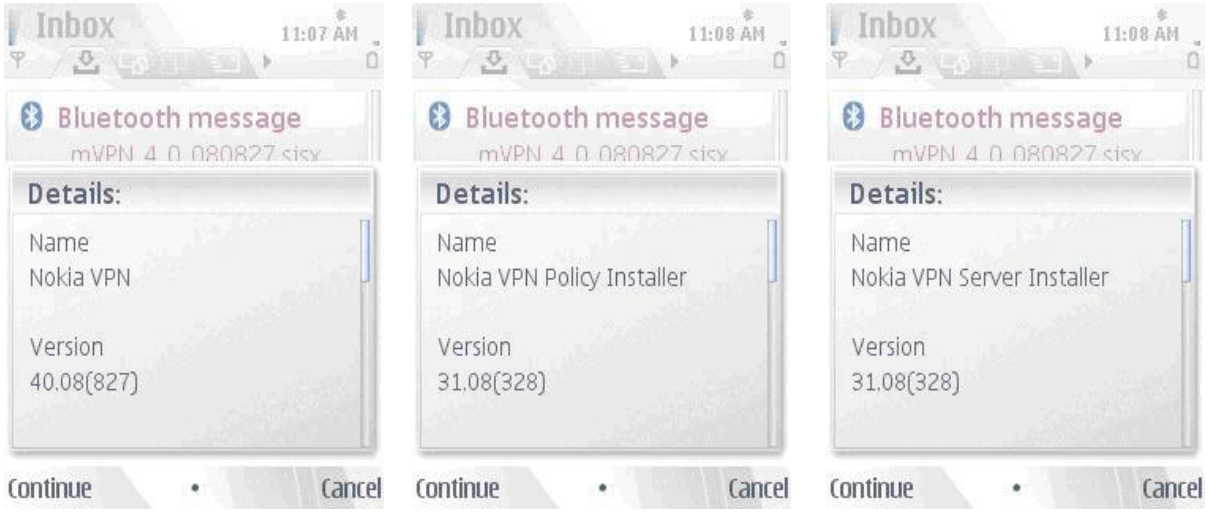


Figure 2 Installation detail dialogs

5. After successful installation, go to Date & Time settings, and make sure the time and date settings on the device are correct (Figure 3 and Figure 4).

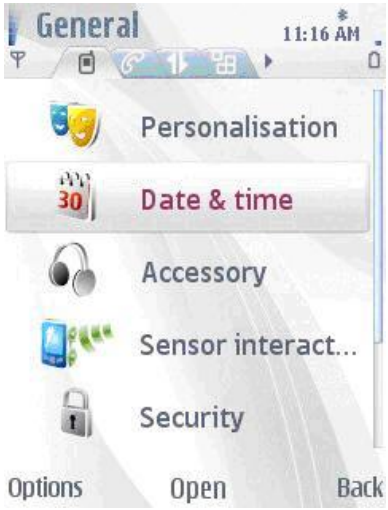


Figure 3 Settings – General – Date & Time

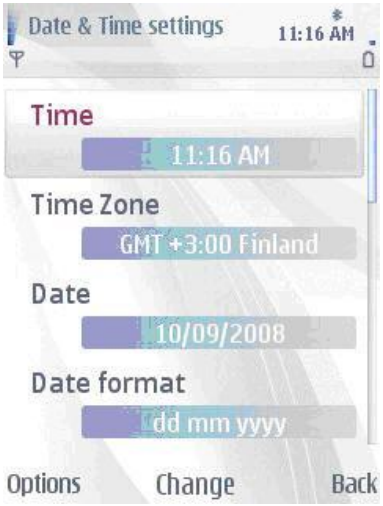


Figure 4 Date & Time settings

6 Configuring Nokia Mobile VPN Client

There are three optional ways how to configure the VPN in the Nokia devices:

- Creating a configuration file and installing it directly to Nokia device via device's user interface
- Using compatible Device Management system based on OMA DM
- Via the legacy Nokia Security Services Manager (NSSM)

The different options are described in the following subchapters. For the first two options the first step is to create a configuration file.

6.1 Creating VPN configuration file

The VPN policy is a pair of text files with extension .pin and .pol. VPN configuration file is a zip file with extension .vpn and it collects together policy files and optional certificate files and private key file.

The recommended way to create VPN configuration file is to use Nokia Mobile VPN Policy Tool [8] which runs on Microsoft Windows.

The policy file specifies the IPsec and IKE parameters and algorithms, VPN gateway FQDN or IP address and other Nokia Mobile VPN Client parameters. The policy file has filename extension .pol and the format is specified in [3].

To create a VPN policy file for Nokia Mobile VPN client, you need to have the following information about your organization's remote access VPN configuration:

- IKE parameters: algorithms, Diffie-Hellman group, authentication method
- IPsec parameters: algorithms, tunnel mode, networks, lifetimes of security associations (SA)
- Optional internal addressing parameters
- When using client certificates, the policy needs to denote whether the user store or device store shall be used to store the certificate

After the configuration has been created, it can be transferred to the device either using device's user interface or via Device Management system.
Note that creating VPN configuration file is not needed when using NSSM.

6.2 Configuring Nokia Mobile VPN Client Via the Device User Interface

This subchapter describes how the VPN configuration file can be transferred to the device and how VPN access point can be configured.

The simplest way to set up a VPN policy, certificates, and a private key via the user interface is to import them from a configuration file (file extension .vpn) with a single installation step. If the device supports the device key store, and if the VPN policy denotes that the device key store shall be used, then the keys will be automatically placed in the device key store.

Transfer the configuration file from PC to device

The configuration file can be installed via the File Manager or from the messaging, if you send the file to the device over Bluetooth or Infrared. After you have sent the file via Bluetooth or Infrared, it will appear in the messaging inbox. Open the file in the Inbox to install the contained VPN policy, certificates, and private key.

Figure 5 shows how a configuration file can be seen in Inbox once it is moved there via Bluetooth. User can open given message and install policy as shown in Figure 6.

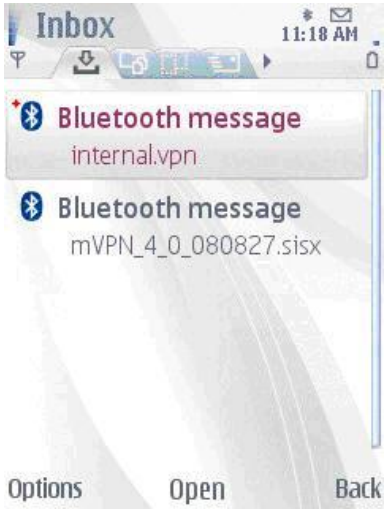


Figure 5 Transfer configuration via Bluetooth

Figure 6 Using Messaging to install a .vpn file

The installed VPN policies will appear in menu Settings – Connection – VPN. Select VPN policies to see the list of installed policies (Figure 7 and Figure 8).

Figure 7 VPN settings in Connection settings

Figure 8 VPN policy view after successful policy installation

Installing VPN Policies, Certificates, and Private Keys Separately

It is also possible to install the policy, certificate, and private key files in separate steps, as shown below. The recommended way is though to bundle certificates in the VPN configuration file as is, or packaged in a PKCS#12 file.

To install a CA certificate with the File Manager, select the CA certificate file as shown in Figure 9. Save the certificate and choose a label for it, as shown in Figure 10. The label is an identifier that is used in the device user interface to refer to the certificate.

Figure 9 Installing a CA certificate via File Manager

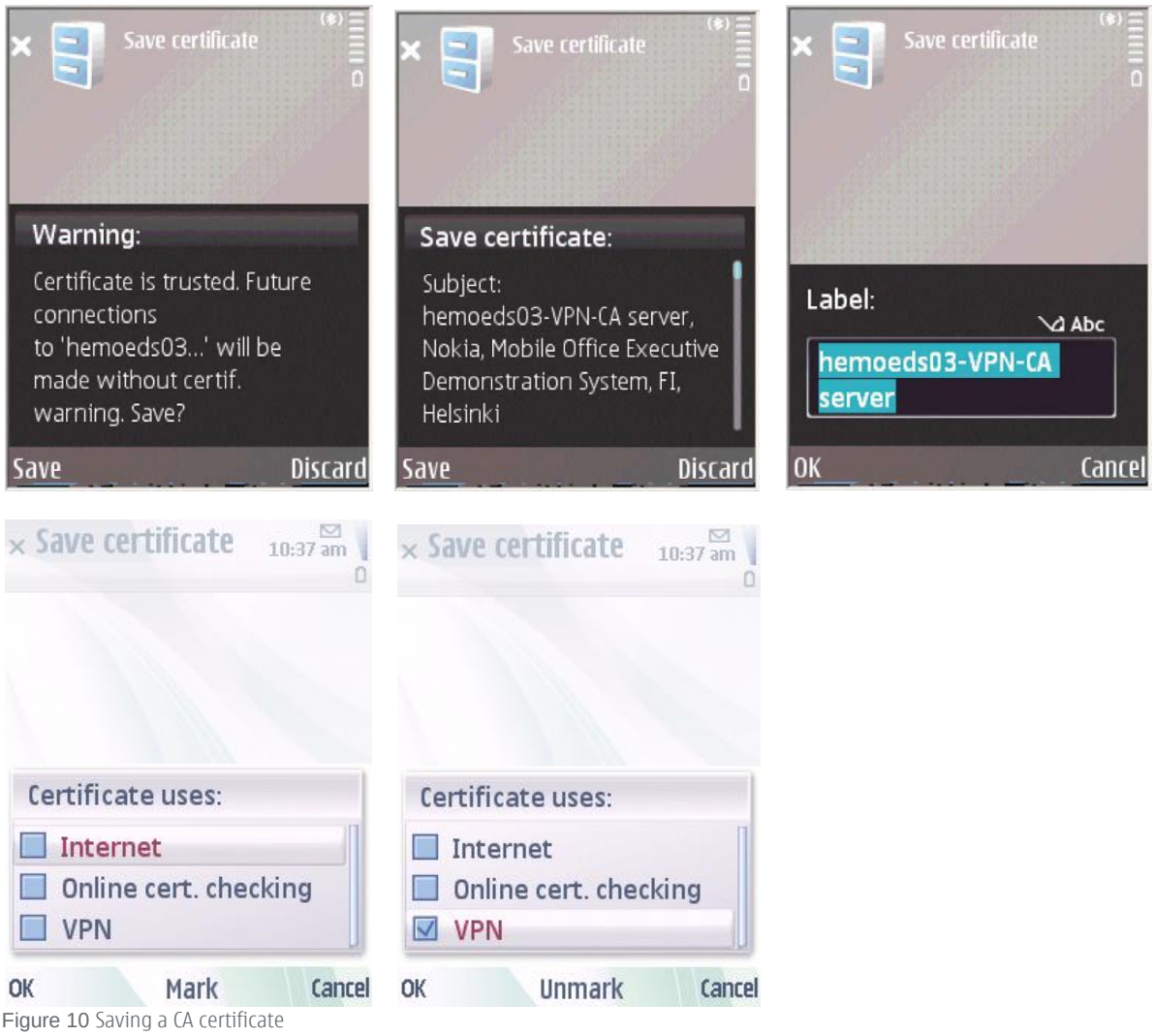


Figure 10 Saving a CA certificate

If you are using client certificate-based authentication and you are not using a VPN configuration file (extension .vpn) to install the client certificate and the private key, then install a key pair and a client certificate from a PKCS#12 file. This is illustrated in the following steps.

1. In the File Manager, open the PKCS#12 file as shown in Figure 11.

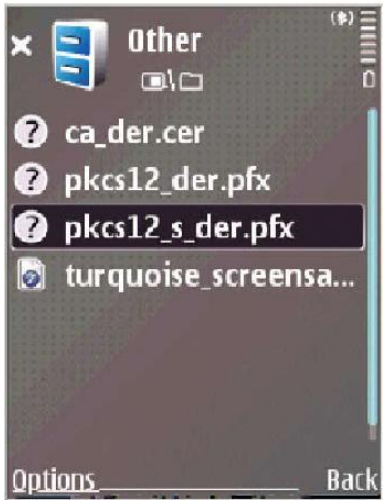


Figure 11 Installing a key pair and a client certificate from a PKCS#12 file

2. The private key included in the PKCS#12 file is protected with a PKCS#12 password. Enter the password to open the file (Figure 12).

Figure 12 PKCS#12 password query

3. The device then shows the contents of the PKCS#12 file (Figure 13). Press "Save" to proceed.

Figure 13 Device displays the contents of a PKCS#12 file

4. The user key store is the default storage for new private keys. When you import the first key to the device, the device asks you to select a password for the user key store (Figure 14). You will later need to enter this password to use the private key for VPN authentication, unless you move the key to the device key store.

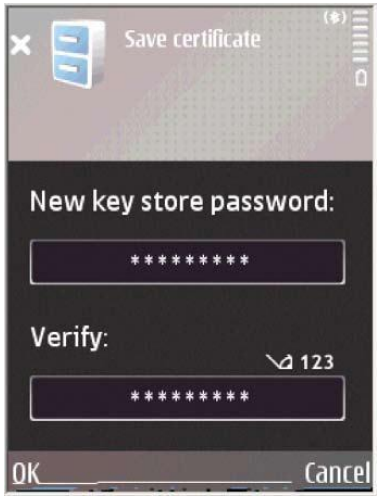


Figure 14 Setting the key store password

5. Figure 15 shows the final steps of saving the contents of a PKCS#12 file. You can select a user interface label for the new client certificate.

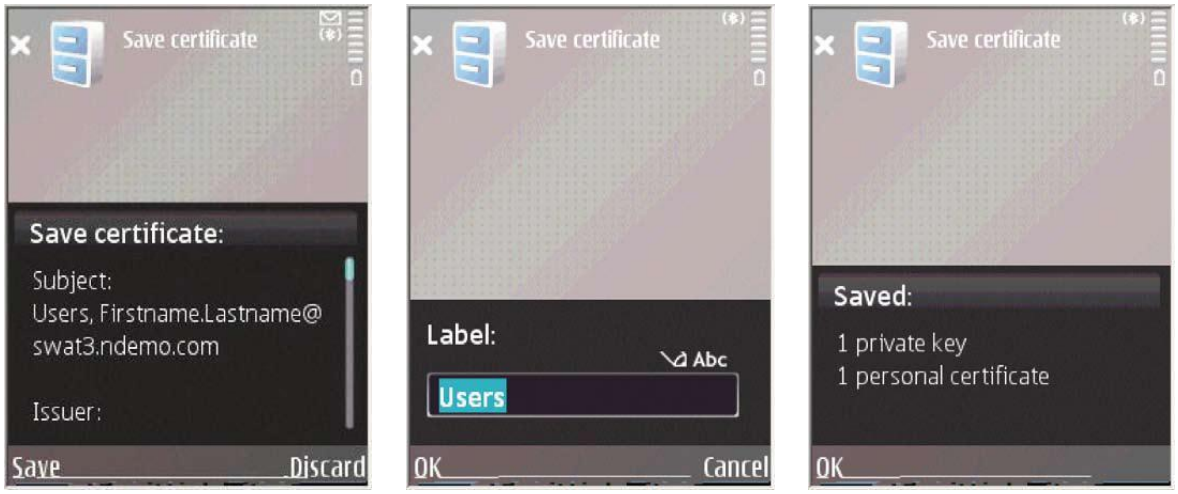


Figure 15 Final steps of saving a PKCS#12 file

6. By default, the use of the new certificate and the associated private key requires the user to enter the key store password. This prompt will occur when the user is establishing a VPN connection. To avoid the password prompt, the certificate can be moved from the user store to the device store. Because the user won't be prompted anymore, it is recommended to activate the device lock when using the device key store. The certificate can be moved from the user store to the device store via Certificate management, which can be found in menu Settings – General – Security – Certificate management. As shown in Figure 16, select "Personal certificates" in the Certificate manager to view certificates. The "Move to Phone certificates" option will move the certificate to the device store.

PLEASE NOTE: Support for the device key store depends on the device.

PLEASE NOTE: The VPN policy file (.pol) needs to indicate which key store is used. To use the device store, your VPN policy must indicate that the device key store shall be used.

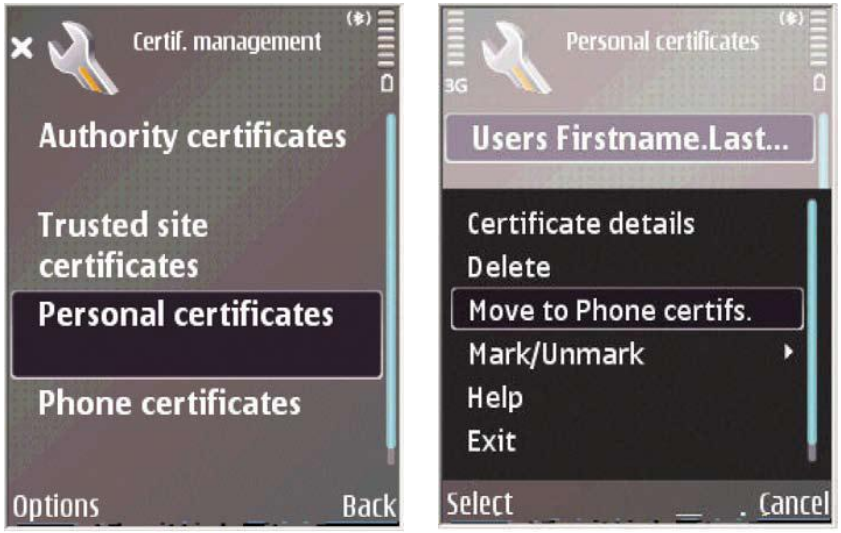


Figure 16 Certificate management

7. To proceed with moving the certificate, click "Yes" to the confirmation question shown in Figure 17. You will need to enter the user key store password in order to unlock the private key.

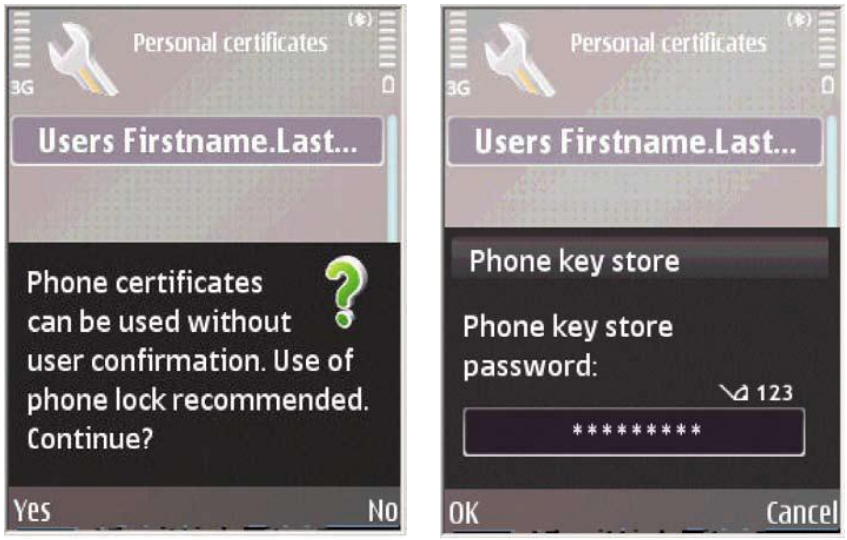


Figure 17 Moving certificate to device store

8. After you have moved the certificate to the device store, it disappears from the list of personal certificates. To view the device certificates, select "Phone certificates" in the Certificate Management main view. (Figure 18)

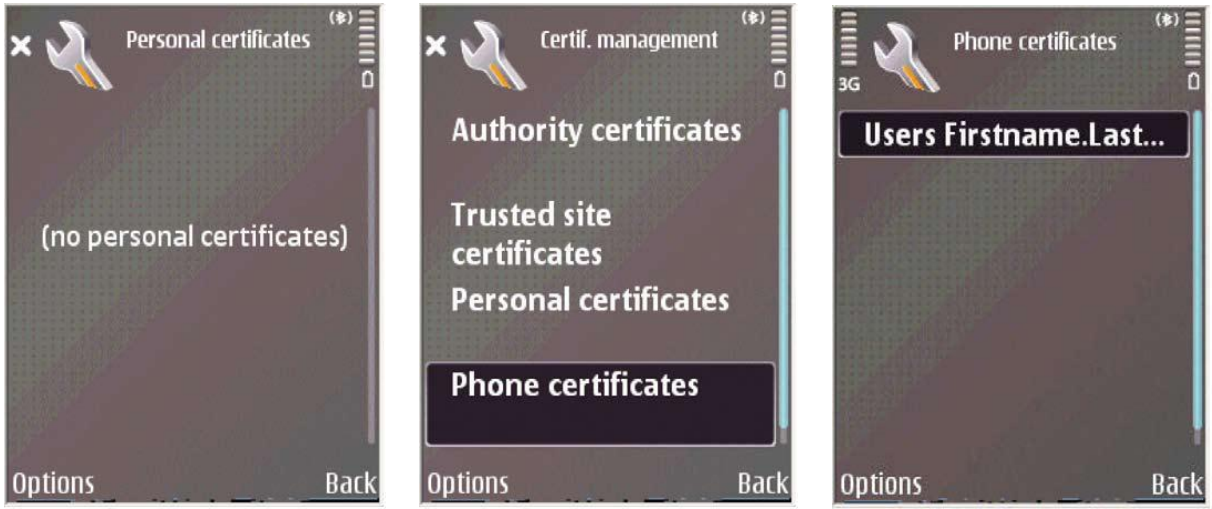


Figure 18 Viewing device certificates

Configuring VPN access points

After installing the certificates and policies, VPN access point is created automatically into Intranet Network destination (Figure 19).

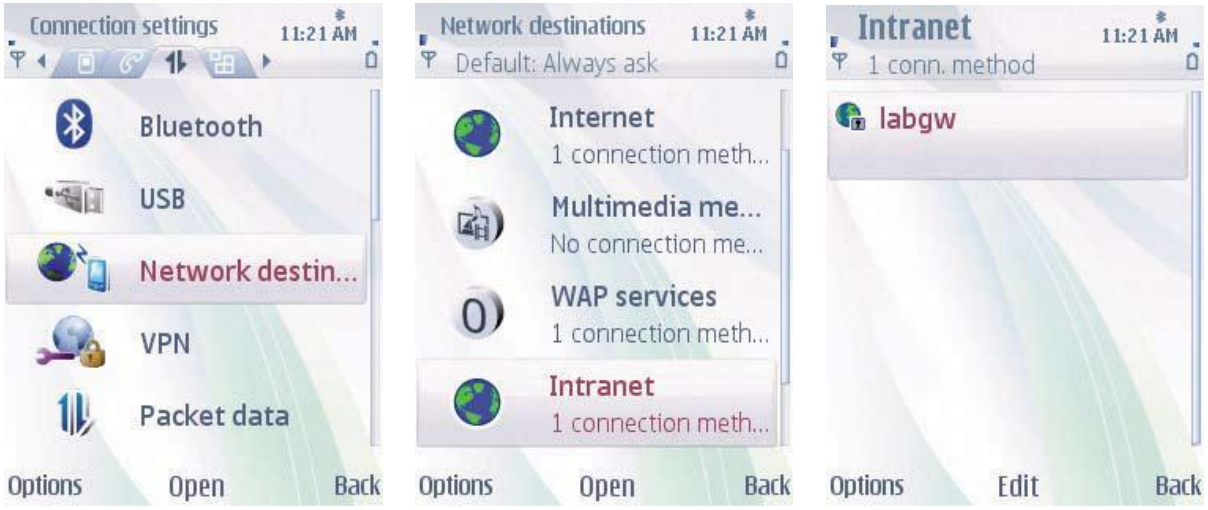


Figure 19 Creating a VPN Internet access point

Optionally, you can configure a web proxy address and port for the new VPN access point.

6.3 Configuring Nokia Mobile VPN Client with OMA Device Management

The recommended way to deploy Nokia Mobile VPN client when there are at least tens of users is to use remote OMA DM solution. Mobile VPN policies, access points, and certificates can be managed over OMA DM similarly as other settings. Once the device has been associated with a device management server, the management of the settings can be made totally transparent to the user. VPN policies can be continuously managed, for example, when your organization's VPN gateway configurations change.

Also in this case the VPN configuration file must be first created as described in chapter 6.1.

Nokia Mobile VPN client comes with OMA DM support for certificates. The certificates are stored in the S60 certificate management so they will be available for other applications besides the mobile VPN client. In addition to CA certificates, user and device certificates can also be managed with OMA DM. The management server can specify which key store shall be used.

For client certificate management with OMA DM, Nokia Mobile VPN client supports two mechanisms:

1. Provisioning of a key pair and a client certificate in PKCS#12 format. The PKCS#12 password is either prompted from the user or provided by the device management server together with the PKCS#12 file.

2. Device management solution requests the device to generate a key pair and a certificate request in PKCS#10 format. The device management solution receives the PKCS#10 file from the device and uses it to obtain a client certificate. The device management server then provisions the certificate to the device.

PLEASE NOTE: The OMA DM PKI management features of Nokia Mobile VPN client only provide means to transport PKCS#12 files, PKCS#10 files, and certificates between the device and the device management solution. For automated enrollment of client certificates, the device management server and the Certificate Authority (CA) need to be integrated. For more information, refer to the documentation of your device management solution. The OMA DM support is specified in [4] and [5].

The following steps illustrate a general OMA DM session from the user's point of view.

1. First, the device receives the device management solution's settings in an SMS (Short message). Open the message and enter the settings' PIN to open the settings; then select "Save" from "Options" to save the setting, as shown in Figure 20. The settings PIN is a security code that the user receives from the administrator.

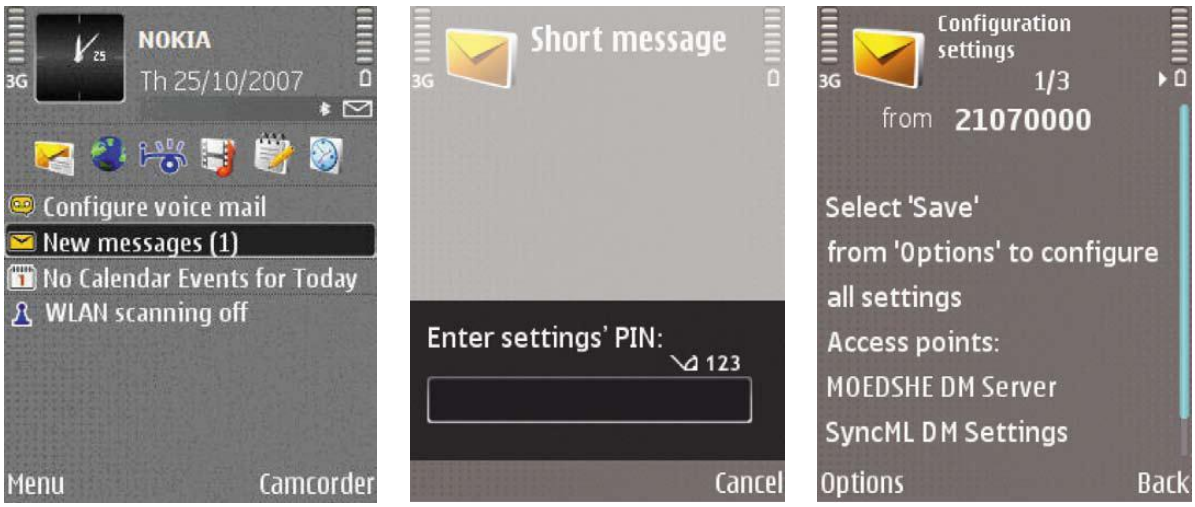


Figure 20 Receiving device management settings

2. When advanced device management is not being used, the user needs to accept all device management sessions, and confirm that an Internet connection can be used. This is illustrated in Figure 21.

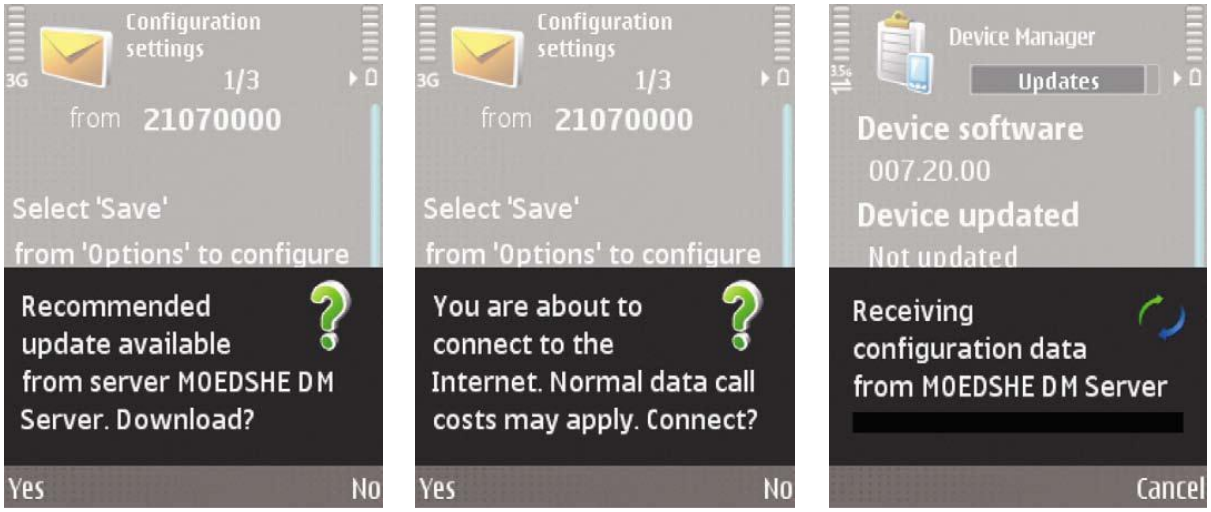


Figure 21 Receiving configuration data from device management server

3. Optional: With advanced device management, the solution can perform silent management operations and enforce security settings. To take advanced device management into use, the user needs to accept a security notification and provide the first four numbers of the server's certificate fingerprint. The IT administrator provides the fingerprint numbers to the users separately to help ensure that the user is associating with a legitimate server. Establishing the trust relationship for advanced device management is illustrated in Figure 22.

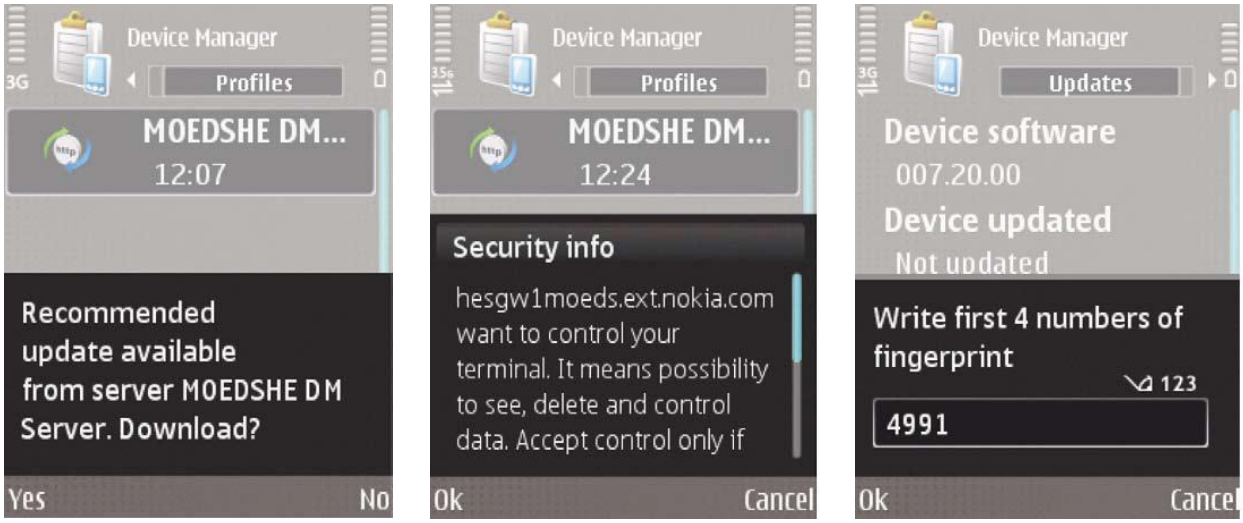


Figure 22 Taking advanced device management into use

6.4 Configuring with Nokia Security Service Manager

Nokia Security Services Manager (SSM) is a dedicated VPN management product by Nokia. Nokia Mobile VPN Client supports Nokia SSM for VPN policy, certificate, and access point management.

Please note that support of Nokia SSM is deprecated in VPN client version 4.2 onward.

Nokia SSM does not support all features that are available via the user interface or via OMA DM. Nokia SSM does not support certificate management with PKCS#12 files, and it always uses the user store of the device for storing keys and certificates.

For more information about Nokia SSM, see [6] and [7].

The device user interface refers to Nokia SSM as a "VPN policy server." VPN policy servers are optional. Manual policy configuration or OMA DM can be used instead.

To configure Nokia Mobile VPN client with Nokia SSM, follow the steps below.

1. Go to menu Settings – Connection – Virtual Private Network, and select VPN policies. As you don't have any VPN policies yet, the device asks you whether to install VPN policies now (Figure 23). Press "Yes" to continue.

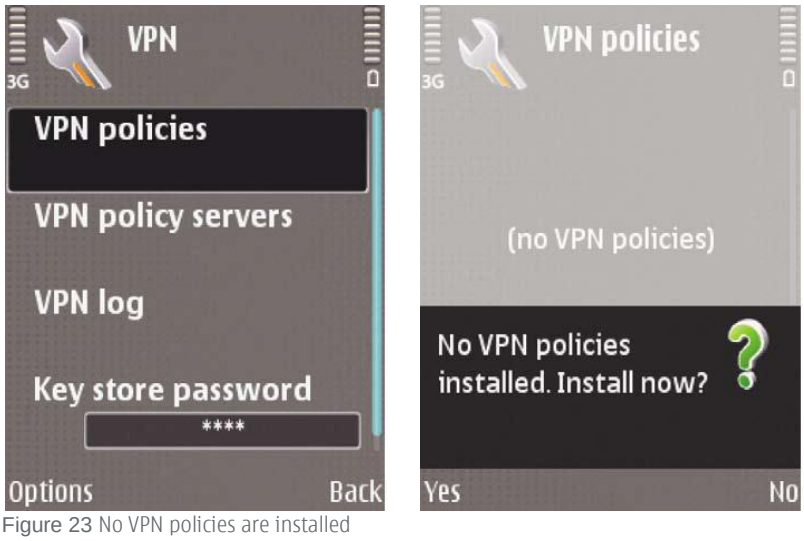


Figure 23 No VPN policies are installed

2. The device then asks you to define a VPN policy server. Press "Yes" to continue, and enter a name, IP address, and an access point. The name is only used in the user interface. Once you have saved the settings, the device asks you whether to synchronize with Nokia SSM. Press "Yes" to continue (Figure 24).

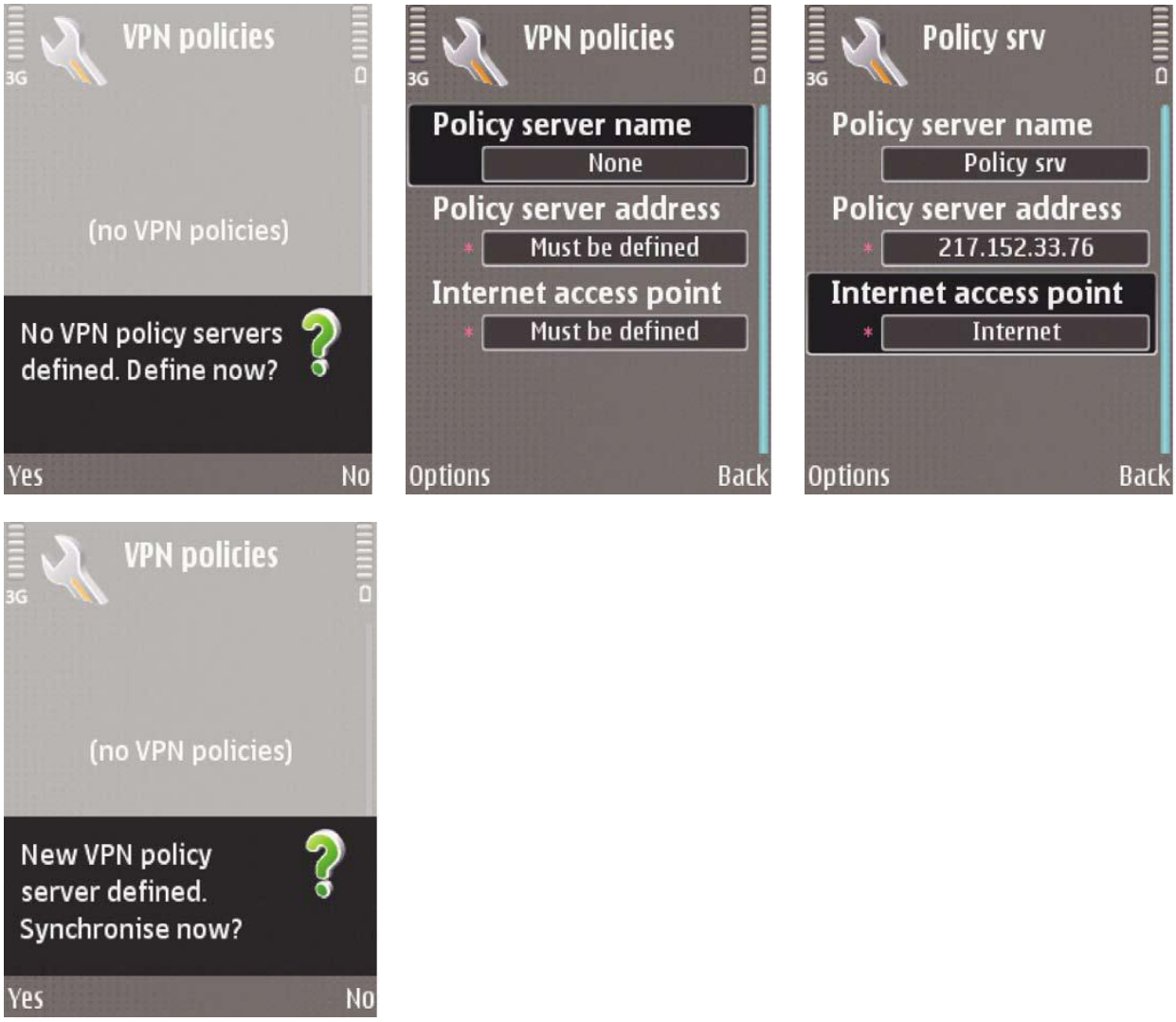


Figure 24 Defining a new VPN policy server

3. On the very first connection with Nokia SSM, the server identity code needs to be verified in order to ensure that the user is associating with a legitimate server. The IT administrator needs to provide the server identity to the user separately, and the user needs to fill in the missing characters of the identity code, as shown in Figure 25.

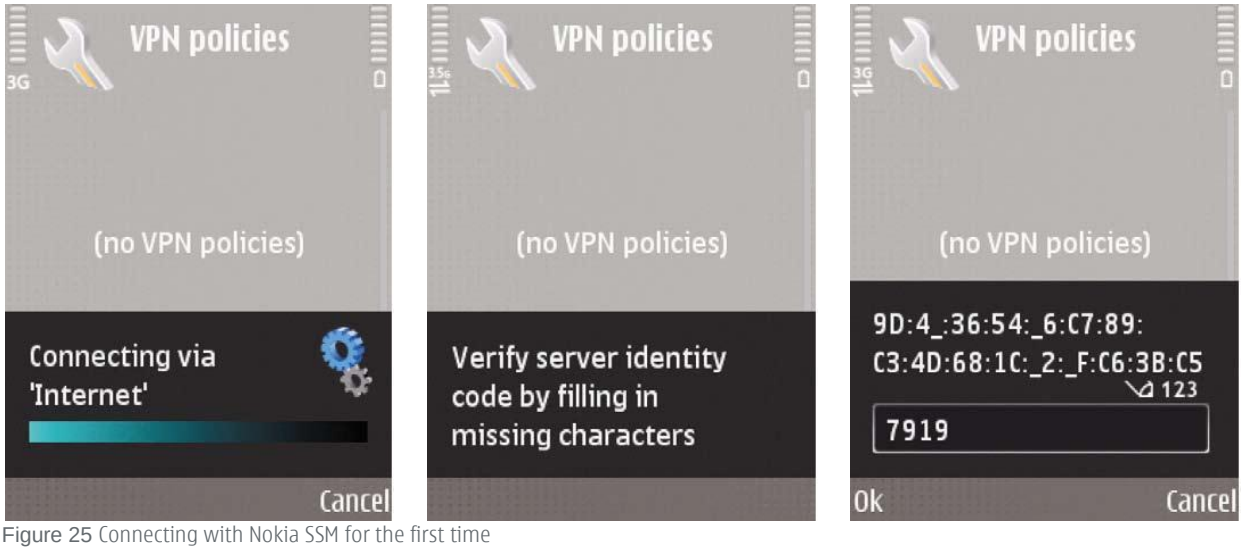


Figure 25 Connecting with Nokia SSM for the first time

4. Next, enter the key store password as shown in Figure 26.

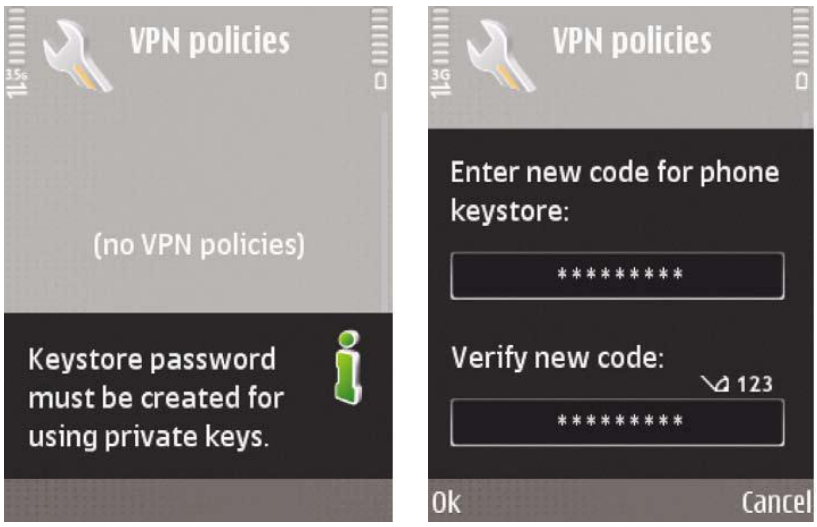


Figure 26 Entering the key store password.

5. The user is authenticated to Nokia SSM with a username and a password. Enter the credentials and press "OK" to continue (Figure 27).

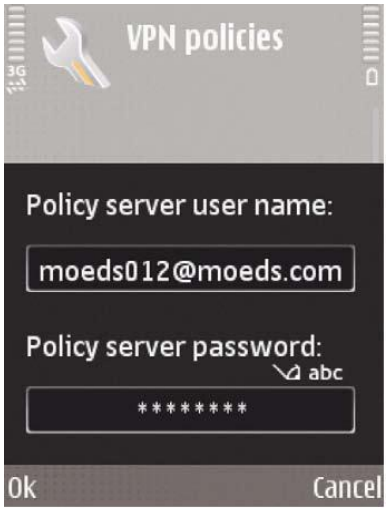


Figure 27 Authenticating to Nokia SSM

6. When the synchronization is completed successfully, the device will be configured with VPN policies, certificates, and VPN access points.

7 Using Nokia Mobile VPN Client

Nokia Mobile VPN client is ready for use once you have successfully configured VPN policies, network destinations, and optionally certificates. To use a VPN connection in applications, configure the application to use a Intranet network destination.

- TIP: The connection setting in many applications can be configured to "always ask." When this option is selected, the application will prompt the user to select the network destination when a connection is being established. The user can then select an Intranet network destination or some other destination for the session.

As far as applications are concerned, VPN access points behave similarly to other access points. For instance, the user selects the Intranet destination used by an application with the same user interface that is used to select ordinary Internet destination. VPN client will start up automatically when the application starts using the network services through the destination. VPN client will, at that point, handle the user authentication and set up the connection through the VPN gateway according to the security policy of the VPN access point. Once the authentication and connection setup has been completed successfully, all Internet Protocol traffic through the Intranet destination will be encrypted.

The VPN access point makes use of the VPN transparent to applications. Applications that do not need VPN access can be used at the same time simply by configuring them to use ordinary Internet destination. This means that, for example, browsing and accessing email can be done through the corporate network using VPN services at the same time as multimedia messaging and Instant Messaging communicate directly over cellular packet data with the servers of the network operator.

PLEASE NOTE: This behavior is limited by the number of simultaneous Packet Data Protocol (PDP) contexts that the network of the device supports.

The VPN connection is closed when the last application that is using it closes its connection.

8 Frequently Asked Questions

Which data bearers can I use for mobile VPN connections?

Mobile VPN can be used with any Internet Protocol (IP) bearer that the device supports, such as packet data, and wireless LAN.

If I receive a voice call or a message during the VPN connection, will the VPN connection be dropped?

In some cases, the VPN connection may be dropped. This may occur, for example, if you are using a packet-data connection in a network that does not support simultaneous data and voice connections.

For which applications can I use the mobile VPN in my Nokia device?

Typically mobile VPN is used for Intranet web browsing, corporate email and corporate VoIP.

Mobile VPN connections are used as Internet access points in the device. In most Internet applications such as email and web browsing, you can use the mobile VPN simply by selecting a VPN Internet access point in the application settings instead of, for example, a direct wireless LAN or packet-data access point.

How can I restore my VPN settings if I need to format the device or upgrade its software?

The recommended way to restore the VPN settings is to install them again using the instructions from your company's IT organization.

How do I know if I have mobile VPN already installed in my device?

Go to menu Settings – Connection. If mobile VPN is already installed, then you should be able to find VPN in this view.

The VPN client seems to consume a lot of battery power in 3G networks. Are there any ways to reduce the power consumption?

The power consumption is increased because of keep-alive messages the device sends for firewall and Network Address Translation (NAT) traversal. In many firewalls and NATs, the expiration timers for mappings are short, i.e., less than one minute. Therefore, the VPN client needs to send frequent keep-alive messages to maintain the mappings. The keep-alive interval is a configurable parameter in the VPN policy. One way to improve the power consumption is to ensure that firewalls and NATs use a long expiration time for IPsec traffic—for example, ten minutes—and then configure the keep-alive interval in the VPN policy to slightly less than half of the expiration interval. See "Recommendations for Reducing Power Consumption of Always-on Applications," available at www.forum.nokia.com, for more discussion on the power consumption of Internet applications.

9 Troubleshooting

9.1 How to Get Support

Please see the Nokia Mobile VPN support documents available on www.nokia.com/mobilevpn.

If the information you are looking for is not found from any of the support documents available you can contact Nokia care.

If you have purchased the VPN backend from Nokia and you have a support agreement you can contact Nokia technical support according to you support agreement.

If contacting to Nokia support please prepare to give detailed information about your company's VPN backend infrastructure, mobile device model and software version, Nokia Mobile VPN client version number and other related information.

For support on Nokia device related features, contact your local Nokia care.

See the Nokia care contact details at: http://www.nokia.com/A4126576

9.2 VPN Log

In troubleshooting cases, view the VPN log file at Settings > Connection > VPN > VPN Log. The log contains a description of the most recent VPN-related events.

9.3 Error codes

The error codes may be shown in dialogs and in VPN Log when an error occurs during configuration phase or usage. See reference document [3] for details of different policy parameters.

Code	Description
-5229	POL file is missing from the policy. See reference document *[3]* for details.
-5230	PIN file is missing from the policy. See reference document *[3]* for details.
-5231	User certificate does not have associated private key or CA certificate format is unexpected (should be BIN).
-5232	Policy which is tried to be accessed has been deleted.
-5233	CA certificate file defined in the POL file is not found. See reference document *[3]* for details.
-5235	User certificate file defined in the POL file is not found. See reference document *[3]* for details.

-5236	Private key file defined in the POL file is not found. See reference document *[3]* for details.
-5237	Policy import operation failed because another import operation is ongoing.
-5238	Key store password change operation failed, because another change password operation is currently ongoing.
-5256	Negotiation with gateway failed.
-5255	ISAKMP section is missing from the policy file or contains invalid parameters.
-5257	IKE negotiation with gateway failed because there was no response.
-5258	IKE negotiation with gateway failed because there was no acceptable proposal.
-5259	IKE negotiation with gateway failed because gateway rejected device's authentication data.
-5260	IKE negotiation with gateway failed because device rejected gateway's authentication data.
-5261	IKE negotiation with gateway failed because needed certificate cannot be found.
-5262	IKE negotiation with gateway failed because the policy was not found.
-5263	Policy parameter MODE has invalid value.
-5264	Policy parameter SEND_NOTIFICATION has invalid value.
-5265	Policy parameter USE_COMMIT has invalid value.
-5266	Policy parameter IPSEC_EXPIRE has invalid value.
-5267	Policy parameter SEND_CERT has invalid value.
-5268	Policy parameter INITIAL_CONTACT has invalid value.
-5269	Policy parameter RESPONDER_LIFETIME has invalid value.
-5270	Policy parameter REPLAY_STATUS has invalid value.
-5271	Policy parameter GROUP_DESCRIPTION_II has invalid value.
-5272	Policy parameter PROPOSALS has invalid value.
-5273	Policy parameter ENC_ALG is either missing or has invalid value.
-5274	Policy parameter AUTH_METHOD is either missing or has invalid value.
-5275	Policy parameter HASH_ALG is either missing or has invalid value.
-5276	Policy parameter GROUP_DESCRIPTION is either missing or has invalid value.
-5277	Policy parameter GROUP_TYPE is either missing or has invalid value.
-5278	Policy parameter LIFETIME_KBYTES has invalid value.
-5279	Policy parameter LIFETIME_SECONDS is either missing or has invalid value.
-5280	Policy parameter PRF has invalid value.
-5281	In policy pre-shared key definition either FORMAT or KEY parameter is missing, KEY parameter has invalid key length or the defined length is too big or HEX formatted key cannot be parsed.
-5282	Policy parameter FORMAT in pre-shared key section has invalid value.
-5283	In Policy CA certificate definition CA count, FORMAT or DATA parameter is either missing or has an invalid value.
-5288	Policy parameter ADDR has invalid value.
-5289	Policy parameter ADDR has invalid net mask value or the net mask is missing.
-5290	Policy parameter ISAKMP_SA_MAX_LIFETIME_SEC has invalid value.
-5291	Policy parameter ISAKMP_SA_MAX_LIFETIME_KB has invalid value.
-5292	Policy parameter ISAKMP_MAX_RETRANS has invalid value.
-5294	Policy parameter CRACK_LAM_TYPE has invalid value.
-5295	Policy parameter USE_INTERNAL_ADDR has invalid value.
-5296	Policy parameter USE_NAT_PROBE has invalid value.

10 Glossary

Abbreviation	Description
CA	Certification Authority
CRACK	Challenge/Response Authentication for Cryptographic Keys
DNS	Domain Name Server. An Internet service that translates domain names such as www.nokia.com into IPv4 addresses like 192.100.124.195.
EAP	Extensible Authentication Protocol
IAP	Internet Access Point. An Internet access point is needed to connect to the Internet.
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange v2
IP	Internet Protocol
IPsec	IP Security Protocol
GPRS	General Packet Radio Service. GPRS is a technology that enables sending and receiving data over a mobile network. GPRS as such is a data bearer that enables wireless access to data networks like the Internet. Examples of applications that use GPRS include the Internet and email.
NAT	Network Address Translation
NSSM	Nokia Security Services Manager (a legacy VPN management solution from Nokia)
OMA	Open Mobile Alliance
OMA DM	Open Mobile Alliance Device Management
PDP	Packet Data Protocol
PFS	Perfect Forward Secrecy
PKCS#10	Standard for certificate requests
PKCS#12	Standard for encapsulating a key pair and a certificate in a file
SA	Security Association
SIM	Subscriber Identity Module
USIM	Universal Subscriber Identity Module (for 3G authentication)
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN / WiFi	Wireless Local Area Network. A local area network in which radio links instead of physical cables are used to connect devices.

Work together. Smarter.

Nokia Inc. 102 Corporate Park Drive, White Plains, NY 10604 USA
Americas Tel: 1 877 997 9199 • Email: usa@nokiaforbusiness.com
Asia Pacific Tel: +65 6588 33 64 • Email: asia@nokiaforbusiness.com
Europe France +33 170 708 166 • UK +44 161 601 8908 • Email: europe@nokiaforbusiness.com
Middle East and Africa Dubai +971 4 3697600 • Email: mea@nokiaforbusiness.com

www.nokiaforbusiness.com

© 2010 Nokia. All rights reserved. Nokia, Nokia Connecting People, Eseries, E52, E55, E71x, E61, E72, and E75 are trademarks or registered trademarks of Nokia Corporation. Check Point, the Check Point logo, VPN-1, and FireWall-1 are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. Other product and company names mentioned herein may be trademarks or trade names of their respective owners. THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES AND IS NOT WARRANTED TO BE ERROR-FREE, NOR IS IT SUBJECT TO ANY OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESSED ORALLY OR IMPLIED IN LAW, INCLUDING IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Nokia specifically disclaims any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. Under no circumstances shall Nokia be responsible for any direct, special, incidental, consequential, or indirect damages howsoever caused. Nokia operates a policy of continuous development. Therefore, we reserve the right to make changes and improvements to any of the products described in this document without prior notice.

NOKIA